PATENT

#8

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Serial No. 09/287,924

Filed: April 7, 1999

For: ENCRYPTING METHOD AND DECRYPTING

Group Art Unit: 2131

Examiner: SEAL, JAMES

VERIFIED TRANSLATION OF PRIORITY DOCUMENT

Honorable Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Sir:

I declare that I can read and speak both the English and Japanese languages, and that I have translated, fully and accurately, the following Japanese application(s) for which priority is claimed:

Copies of my English translation(s) of the above priority application(s) are attached hereto.

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or document or any registration resulting therefrom.

Dated: April 23, 2004

By: Tadashi Shigeyama
Tadashi Shigeyama

7-267252

[Name of Document] Patent Application

[Reference Number] S95082414

[Date of Filing] October 16, 1995

[Administrator] Commissioner of Patent Office, Esq.

[International Patent Classification] G09C 1/00

[Title of the Invention] ENCRYPTING METHOD AND DECRYPTING METHOD

[Number of the Claims] 27

[Inventor]
[Domicile or Residence] c/o SONY CORPORATION
7-35, Kitashinagawa 6-chome,
Shinagawa-ku, Tokyo
Japan
[Name] RYUJI ISHIGURO

[Inventor]
[Domicile or Residence] c/o SONY CORPORATION
7-35, Kitashinagawa 6-chome,
Shinagawa-ku, Tokyo
Japan
[Name] MASAFUMI MINAMI

[Patent Applicant]

[Identification Number] 000002185

P7-267252

[Name or Appellation] SONY CORPORATION

[Representative] Nobuyuki Idei

[Agent]

[Identification Number] 100080883

[Patent attorney]

[Name or Appellation] Hidemori Matsukuma

[Phone Number] 03-3343-5821

[Indication of Fee]

[Ledger Number] 012645

[Amount of Payment] 21,000 yen

[List of Attached Things]

[Name of a Thing] Specification 1

[Name of a Thing] Drawings 1

[Name of a Thing] Abstract 1

[Number of a Comprehensive Power of Attorney] 9006428

[Title of Document] Specification

[Title of the Invention] ENCRYPTING METHOD AND DECRYPTING METHOD

[Scope of Claim for a Patent]

[claim 1] An encrypting method comprising the steps of: obtaining an encryption key based on inherent information inherent in a recording medium; and encrypting information data to be recorded on said recording medium based on said encryption key.

[claim 2] In an encrypting method according to claim 1, an encrypting method characterized in that said inherent information inherent in said recording medium is information signal inherent for the recording medium to be recorded on said recording medium.

[claim 3] In an encrypting method according to claim 1, an encrypting method characterized in that said information signal inherent for the recording medium to be recorded on said recording medium is random data to be inserted into a predetermined portion of said encrypted information data to be recorded on said recording medium.

[claim 4] In an encrypting method according to claim 3, an encrypting method characterized in that a file of said encrypted information

data and a file indicative of the portion of random data to be inserted into a predetermined portion of said encrypted information data recorded on said recording medium are recorded on said recording medium.

[claim 5] A decrypting method characterized by obtaining an encryption key based on random data to be inserted into a predetermined portion of said encrypted information data to be recorded on a recording medium; reproducing a file of information data encrypted by said encryption key and a file indicative of the portion of random data inserted into a predetermined portion of encrypted information data recorded on said recording medium from a recording medium recorded with the file of information data encrypted by said encryption key and the file indicative of a predetermined portion of random data inserted into a predetermined portion of encrypted information data recorded on said recording medium; detecting said random data from said reproduced encrypted information data based on the reproduced file indicative of the portion of random data inserted into a predetermined portion of encrypted information data recorded on said

recording medium; generating a decryption key from said detected random data; and decrypting said encrypted information data of said reproduced information-data file by using said decryption key.

[claim 6] In an encrypting method according to claim 2, an encrypting method characterized in that said inherent information inherent in the recording medium to be recorded on said recording medium is a wobbling frequency of a predetermine portion of information data to be recorded on said recording medium.

[claim 7] In an encrypting method according to claim 6, an encrypting method characterized in that a file of said encrypted information data and a file indicative of the portion of the wobbling frequency to be inserted into a predetermined portion of said encrypted information data to be recorded on said recording medium are recorded on said recording medium.

[claim 8] A decrypting method characterized by obtaining an encryption key based on a wobbling frequency of a predetermined portion of information data to be recorded on a recording medium; reproducing a file of information data encrypted by said encryption key and a

file indicative of a predetermined portion of encrypted information data to be recorded on said recording medium from a recording medium recorded with the file of information data encrypted by said encryption key and the file indicative of a predetermined portion of encrypted information data to be recorded on said recording medium; detecting a wobbling frequency of a predetermined portion of said detected encrypted information data based on the reproduced file of a predetermined portion of encrypted information data ; generating a decryption key from said detected wobbling frequency; and decrypting said encrypted information data of said reproduced encrypted information-data file by using said decryption key.

[claim 9] In an encrypting method according to claim 1, an encrypting method characterized in that said recording medium is a recording medium of a disc shape and said information inherent in said recording medium is a physical information to be formed said recording medium.

[claim 10] In an encrypting method according to claim 9, an encrypting method characterized in that said physical information is a frequency of a predetermined portion of a wobbled pre groove or a wobbled land

portion to be formed on said recording medium.

[claim 11] In an encrypting method according to claim 9, an encrypting method characterized in that said a file of said encrypted information data and a file indicative of a predetermined portion of a frequency at a predetermined portion of a wobbled pre groove or a wobbled land portion to be formed on said recording medium are recorded on said recording medium.

[claim 12] A decrypting method characterized by obtaining an encryption key based on a frequency of a predetermined portion of a wobbling-shaped pre groove or a wobbling-shaped land portion to be formed on a recording medium; reproducing the file of said encrypted information data and the file indicative of a predetermined portion of a wobbling-shaped pre groove or a wobbling-shaped land portion to be formed on a recording medium from a recording medium recorded with a file of information data encrypted by using an encryption key and a file indicative of a predetermined portion of the wobbling-shaped pre groove or the wobbling-shaped land portion to be formed on a recording medium; detecting the wobbling frequency

of a predetermined portion of the pre groove or land portion formed on said recording medium based on said reproduced file of a predetermined portion of said pre groove or land portion; generating a decryption key from the detected wobbling frequency; and decrypting said encrypted information data by using said decryption key.

[claim 13] In an encrypting method according to claim 3, an encrypting method characterized in that said random data is random data selected from a predetermined portion of a random file generated by a predetermined pseudo random generator.

[claim 14] In an encrypting method according to claim 13, an encrypting method characterized in that a information-data file encrypted by said encryption key, a file indicative of said predetermined portion of said random file formed of said random data and said random file are recorded on said recording medium.

[claim 15] A decrypting method characterized by obtaining an encryption key based on random data selected from a predetermined portion of a random file generated by a pseudo random generator; reproducing a file of said encrypted information data, a file

indicative of said predetermined portion of said random file from recording medium recorded with a file of information data encrypted by said encryption key generated, a file indicative of said predetermined portion of said random file; generating a decryption key from random data obtained from a file indicative of a predetermined portion of said random file of said reproduced random data and obtained from said random file; and decrypting the encrypted information data of a file of said reproduced encrypted information data by using said decryption key.

[claim 16] An encrypting method characterized in that information data to be recorded on a recording medium are encrypted by using a first encryption key generated from information inherent in said recording medium and a third encryption key generated from a second encryption key independent of said first encryption key.

[claim 17] A decrypting method characterized by generating a first decryption key from inherent information in a recording medium where encrypted information data are recorded by using a first encryption key generated from information inherent in said recording medium and

a third encryption key generated from a second encryption key independent of said first key; generating a third decryption key from a second decryption key obtained from a key medium provided with a second decryption key related to said second encryption key and from said first key; and decrypting the encrypted information data reproduced from said recording medium by using said third decryption key.

[claim 18] In an decrypting method according to claim 17, an decrypting method characterized in that said key medium is a card where said second decryption key is recorded magnetically or optically.

[claim 19] In an decrypting method according to claim 17, an decrypting method characterized in that said key medium comprises a memory storing said second decryption key.

[claim 20] In a decrypting method according to claim 19, a decrypting method characterized in that said key medium is a card.

[claim 21] In an decrypting method according to claim 17, an decrypting method characterized in that said key medium is a print medium where said second decryption key is printed.

[claim 22] In a decrypting method according to claim 21, a decrypting method characterized in that said print medium is a card.

[claim 23] In a decrypting method according to claim 21, a decrypting method characterized in that said print medium is said recording medium itself.

[claim 24] In an encrypting method according to claim 2, an encrypting method characterized in that said recording medium is a disc shaped recording medium.

[claim 25] In an encrypting method according to claim 2, an encrypting method characterized in that said recording medium is a tape shaped recording medium.

[claim 26] In an encrypting method according to claim 1, an encrypting method characterized in that said information data are video data.

[claim 27] In an encrypting method according to claim 1, an encrypting method characterized in that said information data are audio data.

[Detailed Description of the Invention]

[0001]

[Technical Field Pertinent to the Invention]

The present invention relates to encrypting method of information data such video signals, audio signals, data signals or the like and decrypting method of information data such respectively encrypted video signals, audio signals, data signals or the like.

[0002]

[Prior Art]

In the prior art encrypting method and decrypting method, complicated encrypting apparatus and decrypting apparatus were necessary respectively.

[0003]

[Problem to be solved by the Invention]

In view of such aspect, it is an object of the present invention to provide encrypting method where the constitution of the encrypting apparatus becomes simple, a strong copy protect can be effected on the information data recorded on a recording medium and at the same time the constitution of the decrypting apparatus becomes simple.

[0004]

The present invention is to propose decrypting method where

information data encrypted by the encrypting method according to the present invention.

[0005]

[Means for solving the Problem]

According to a first encrypting method, an encryption key is obtained based on inherent information inherent in a recording medium and information data to be recorded on the recording medium are encrypted based on the encryption key.

[0006]

[Mode for Carrying Out the Invention]

Hereinafter, several exemplified embodiments of the present invention will be explained with reference to the accompanying drawings. Information data used in the exemplified embodiments are video signal (digital video signal), audio signal (digital audio signal), data signal and so on. It is possible to use, for recording media on which encrypted information data to be decrypted are recorded, disc-like recording media such as optical discs, magneto-optical discs and magnetic discs (flexible discs, hard discs, etc.) and

tape-like recording media such as magnetic tapes or the like. These recording media on which encrypted information data to be decrypted are recorded are slave recording media a large number of which are produced by duplication of a master disc, a master magnetic tape or the like. It is possible to apply as encrypting method such as coding, scrambling, shuffling, encoding according to a so-called MPEG system and encoding according to a so-called JPEG system, and in accordance with those and accordingly as decrypting method, it becomes possible to apply de-scrambling, de-shuffling, decoding according to the MPEG system, decoding according to the JPEG system and so on.

[0007]

It should be noted that corresponding portions in Figs. 1, 5, 7 and 11 which show the encrypting apparatus and decrypting apparatus respectively are put with same reference numerals and overlapped explanation thereof will be partially omitted. Also, an encrypting apparatus 1 in each of the drawings is provided in a record medium manufacturing apparatus and a decrypting apparatus 14 is provided in a record medium reproducing apparatus. Further, these encrypting

apparatus 1 and decrypting apparatus 14 are provided with microcomputers respectively and some of means of the drawings could be functions of the microcomputers.

[0008]

An encrypting apparatus and a decrypting apparatus which are applied with an encrypting method and a decrypting method of exemplified embodiments according to the present invention will be shown with reference to FIG. 1. The reference numeral 1 shows an encrypting apparatus as a whole and the reference numeral 14 shows a decrypting apparatus as a whole.

[0009]

First, an encrypting apparatus 1 and encrypting method will be explained with reference to FIGS. 1 and 2. information data (plain text) from a data generating means 2 consisting of a reproducing apparatus or the like for reproducing the information data from a recording tape on which information data (e.g. digital video information of digital audio information) are recorded are supplied to an encrypting means 3 so as to obtain encrypted information data

(cryptogram) thereof.

[0010]

The reference numeral 5 is a generating means of an information signal inherent in a recording medium and random data (random number data and the like) are used as this information signal inherent in a recording medium where the random data are inserted to a predetermined area in the encrypted information data, for example, in an application area of a primary volume descriptor of ISO9660, in a reserved area stated from sector 0 or the like and recorded temporarily on a hard disc by using a recording means (including a magnetic head, an amplifier and the like) 7 though they are finally recorded on a master disc 12.

[0011]

The reference numeral 6 is a file forming means for forming a file indicative of a predetermined portion of an encrypted information data and forms a file of a sector number or an offset (byte number in a sector) from a predetermined byte number to another predetermined byte number in the same sector or over different sectors of the random

data recorded on the master disc 12 with being inserted in the above mentioned encrypted information data. Then, the file indicative of a predetermined portion of the information data is also inserted into a predetermined area in the encrypted information data, which means that it is temporarily recorded on a hard disc 8 by using the recording means 7 though it is finally recorded on the master disc 12.

[0012]

FIG. 2 is referred and with respect to the random data (random-number data) for obtaining an inherent value (encryption key), it is determined to gather them from a predetermined portion, that is, from which portion of the random data themselves in the encrypted information data including the random data which are recorded on the master disc 10 or random data of a plurality of portions (step ST-1), and a file indicative of the predetermined portions is formed in the file forming unit 6. As shown in FIG. 3, for example, the file (digest method file) is, for example, formed of a table including a large number of offsets (offset numbers) of n sectors from the sector number 1 to the sector number n (here, n is the number of about several tens),

and as shown in FIG. 4, the table designates data from a certain offset in a sector of the sector number 1 to another certain offset therein and data from a certain offset in a sector of the sector number 2 to another certain offset therein where it is recorded by the recording means 7 on the hard disc 8.

[0013]

With respect to the determined digest method file, the random data from a certain offset in a sector of the sector number 1 to another certain offset therein and data from a certain offset in a sector of the sector number 2 to another certain offset therein which are recorded on the hard disc 8 are gathered (step ST-2), and the random data (random-number data) are reproduced by the reproducing means (including a magnetic head, an amplifier, etc.) 9 and supplied to the encryption-key generating means 4 and then, these random data are subjected to a predetermined calculation so as to generate the encryption key (inherent value) (disc digest) as shown in FIG. 4 (step ST-3). The encryption key is supplied to the encryption-key generating means 3 so as to encrypt the information data supplied from the

information data generating means 2 (step ST-4) and these encrypted information data are recorded on the hard disc 8 by using the recording means 7.

[0014]

The encrypted information data, the information data inherent in the recording medium and the digest method file indicative of the encrypted predetermined portion which are recorded on the hard disc 8 are reproduced in the reproducing means 9 and supplied to the formatting means 10 so as to be formatted and a pre-master image is generated (step ST-5) where the pre-master image, that is, the formatting signal is temporarily recorded on the hard disc by using the recording means 7 and they are reproduced by using the reproducing means 9 so as to be recorded on the master disc 12 by using the recording means 11 (including a magnetic head, an amplifier, etc.). It should be noted that it is possible to record the pre-master image, that is, the formatting signal from the formatting means 10 directly on the master disc 12 by using the recording means 11.

[0015]

Then, the disc producing apparatus 13 employs the master disc 12 as an original disc to reproduce a large number of the discs (slave discs) (optical disc, magneto-optical disc, etc.) 15. Here, if the recording medium is a magnetic tape, a transfer apparatus may be employed to transfer recorded signals of the master magnetic tape to a large number of slave magnetic tapes.

[0016]

Next, the decrypting apparatus 14 and the decrypting method will be explained. The signals recorded on the disc 15 are reproduced by the reproducing means 16 and the encrypted information data in the reproduced signals are supplied to the decrypting means 17 and the file of the random data and the digest method file are supplied to the decryption-key generating means 18 owing to the fact that gate signals are supplied from the decryption-key generating means 18 to the reproducing means 16.

[0017]

In the decryption-key generating means 18, the random data from the certain offset to another certain offset in the sector of the

sector number 1 and the random data from the certain offset to another certain offset in the sector of the sector number 2 which are designated by the digest method file in the random data are extracted, and the decryption key corresponding to the original encryption key is generated from the random data are subjected to the predetermined calculation or from the random data itself and is supplied to the decryption-key generating means 17, and the encrypted information data (cryptogram) are decrypted to the original information data (plain text) by means of the decryption key and outputted to the output terminal 19.

[0018]

In the above mentioned encrypting apparatus 1, it is possible for the generating means 5 to generate signals such that if pit strings of the recording signal are recorded on the track of the master disc 12 in a wobbled fashion, a wobbling signal indicative of the wobbling of the pit strings of the recording signal to be recorded on the master disc 12 is generated instead of aforementioned random data and if a track on which the recording signal of the master disc 12 is to

be recorded is a wobbling shaped pre groove or a wobbling shaped land portion, the wobbling signal corresponding to the pre groove or the land portion is generated as the information signal inherent in the recording medium.

[0019]

In this case, in the decrypting apparatus 14, a wobbling frequency of the pre groove or the land portion corresponding to the predetermined portion of the recording signal on the disc 15 is detected by using the decryption-key generating means 18, and the decryption key corresponding to the original encryption key is generated by subjecting a predetermined calculation to the wobbling frequency or based on the data itself corresponding to the wobbling frequency and supplied to the decrypting means 17 where the encrypted information data (cryptogram) are decrypted to the original information data (plain text) by means of the decryption key.

[0020]

Here, in a case when the information inherent in the recording medium is physical information to be recorded on the recording medium,

more specifically in a case when, for example, it is a wobbling shaped pre groove or land portion of the recording medium, the recording medium has a considerable thickness and is to be a comparatively rigid substrate such as an optical disc, a magneto-optical disc, a hard disc or the like.

[0021]

Further exemplified embodiments of the encrypting apparatus, the encrypting method, the decrypting apparatus and the decrypting method will be explained with reference to FIGS. 5 and 6. In the encrypting apparatus 1, random data (random number data) are generated from the pseudo random data generator whose indication is omitted by using the random file forming means 20 and a random file including random data of, for example, several k-bytes or larger is generated (step ST-1) and the random file is recorded on the on the hard disk 8 by using the recording means 7.

[0022]

Random-number data (random data) for obtaining an inherent value (encryption key) are determined to be gathered from which portions

of the random data of the random file, that is, whether only the random data the random data from a certain offset number to another offset number or the random data formed of a plurality of certain portions are gathered, and a file (digest method file) indicative of the determined predetermined portions are formed by a file forming means 21 for forming a file indicative of the predetermined portions (step ST-2), and the formed file is recorded temporarily on the hard disc 8 through the recording means 7 and finally recorded on the master disc 12.

[0023]

Only the random data from aforesaid certain offset address to another certain offset address or the random data or the random data of a plurality of the predetermined portions are gathered and these random data (random number data) which are recorded on the hard disc 8 are reproduced by the reproducing means 9 and supplied to the encryption-key generating means 4 where the encryption key (inherent value) (disc digest) is generated from the random data itself or the random data subjected to the calculation (step ST-3).

[0024]

The position where the random file is allocated in the master disc 12 is calculated, that is, there is calculated an offset value (offset number) of a predetermined sector number obtained when the random file is inserted into the encrypted information data recorded on the hard disc 8 and then recorded on the master disc 12, and the offset value is added to the offset number (offset value) designated by the digest method file (step ST-4) so that the digest method file is modified.

[0025]

The encryption key (the inherent value) (disc digest) generated in the encryption-key generating means 4 is supplied to the encrypting means 3 and the information data supplied from the information data generating means 2 are encrypted (step ST-5), and the encrypted information data are recorded on the hard disc 8 by using the recording means 7.

[0026]

The reproducing means 9 reproduces the encrypted information

data, the information signal inherent in the recording medium and the digest method file indicative of the predetermined encrypted portion which are recorded on the hard disc 8 are reproduced by the reproducing means 9 and supplied to the formatting means 10 to be formatted, and the pre-master image is produced (step ST-6) where the pre-master image, that is, the formatting signal is recorded on the hard disc 8 temporarily by using the recording means 7 and it is reproduced by using the reproducing means 9, and the reproduced pre-master image or the pre-master image from the formatting means 10 is recorded on the master disc 12.

[0027]

Then, a large number of the discs (slave discs) 15 are duplicated according to the disc producing apparatus 13 by employing the master disc 12 as the original disc. The explanation of the encrypting apparatus 1, the encrypting method and others is similar as in the case of FIGS. 1 and 2.

[0028]

In the decryption-key generating means 18, the random data,

designated by the digest method file, of a portion from the certain offset to another certain offset in the sector of the certain sector number and of another portion from the certain offset to another certain offset are extracted from the reproduced encrypted information data, and the decryption key corresponding to the original encryption key is generated by subjecting the random data to the predetermined calculation or based on the random data itself and supplied to the decrypting means 17 to be decrypted from the encrypted information data (cryptogram) to the original information data (plain text). The explanation of the decrypting apparatus 14, the decrypting method and others is similar as in the case of FIG. 1.

[0029]

Still further exemplified embodiments of the encrypting apparatus 1, the encrypting method, the decrypting apparatus 14 and the decrypting method will be explained with reference to FIGS. 7, 8, 9 and 10. First, the encrypting apparatus 1 and the encrypting method will be explained with reference to FIGS. 7, 8 and 10. In the encrypting apparatus 1, distribution-key data are determined and

registered in a memory (a semiconductor memory) in the encryption-key generating means 4 (step ST-1). Here, a CPU (including a memory) may be used instead of the memory. Similarly as in the case of FIGS. 1 and 2, the information inherent in the disc is gathered and the disc digest (key) is generated by subjecting a predetermined calculation thereto (step ST-2). In the encryption-key generating means 4, the distribution-key and the disc digest are subjected to a predetermined calculation, for example, exclusive-OR so as to obtain a work key (step ST-3) and the work key is supplied to the encrypting means 3, the information data are encrypted (step ST-4) and they are recorded in the hard disc by using the recording means 7. The explanation of the encrypting apparatus 1, the encrypting method and others is similar as in the case of FIGS. 1 and 2.

[0030]

The reference numeral 23 designates a key medium provided with a distribution key (distribution key data) and the key medium 23 may be arranged such that the distribution key (distribution key data) may be printed in the form of Arabic numerals, alphabets, symbols,

bar codes, other codes similar to the bar codes or the like and the key medium 23 may includes a card or the disc 15 itself. Also, the key medium 23 may includes a memory such as a semiconductor memory which stores the distribution key (distribution key data) or a CPU including a memory. Further, the key medium 23 provided with the memory or the CPU may be a card. Furthermore, the key medium 23 may be arranged such that the distribution key (distribution key data) is recorded thereon magnetically or optically. Such key medium 23 is to be sold on a market together with a reproducing apparatus for reproducing the disc 15 or solely.

[0031]

The key of the key medium is obtained (step ST-1) and this is read out by a readout means (optical readout means, memory readout means, etc.) 22 and supplied to the decryption-key generating means 18. In the decryption-key generating means 18, similarly as in the case of FIGS. 1 and 2, the disc digest (key) corresponding to the original disc digest (key) is obtained by gathering and calculating the information inherent in the disc (step ST-2), and in the

decryption-key generating means 18, a predetermined calculation, for example, exclusive-OR between the disc digest (key) and the distribution key is performed for obtaining the work key (step ST-3), and the work key is supplied to the decrypting means 17 as a decrypting key. The decrypting key 17 decrypts the encrypted information data supplied from the reproducing means 16 by using the decryption key supplied from the decryption-key generating means 18 and outputs them through the output terminal 19. The explanation of the decrypting apparatus 14, the decrypting method and others is similar as in the case of FIG. 1.

[0032]

FIG. 11 shows further exemplified embodiment of the encrypting apparatus 1 and the decrypting apparatus 14 where the generating means 5 and the file forming means 6 of FIG. 7 are replaced by the random file forming means 20 and the file forming means 21 respectively. It should be noted that with respect to the explanation of the encrypting apparatus 1, the encrypting method, the decrypting apparatus 14 and the decrypting method I FIG. 11, the explanation

of FIGS. 1 and 2, the explanation of FIGS. 5 and 6 and the explanation of FIGS. 7 to 10 can be similarly applied, so that overlapping explanation will be omitted.

[0033]

It should be noted in each exemplified example mentioned above that, when it is tried to dub information data from the recording medium, it is made impossible to decrypt the encrypted information data by using the decryption key or to output the decrypted information data (especially in a state of digital data) which are obtained by decrypting them to a line-out.

[0034]

The present invention can be utilized for communication such as wire communication (communication through an electric cable, an optical fiber cable or the like), wireless communication (communication utilizing electric waves, light, sound waves or the like), or the like and in this case, it should be read/replaced in the detailed explanation of the invention from "information signal inherent in the recording medium to be recorded on the recording

medium" to "information signal inherent in the transmission signal", from "recording" to "transmitting", from "reproducing" to "receiving" and from "recording medium manufacturing apparatus" to "transmitting apparatus" respectively.

[0035]

[Effect of the Invention]

According to the present first invention, since an encryption key based on inherent information inherent in a recording medium is obtained and information data to be recorded on the recording medium is encrypted based on the encryption key, the constitution of the encrypting apparatus becomes simple, and it is possible to effect a strong copy protect on the information data which is recorded on a recording medium and at the same time to obtain a decrypting method where the constitution of the decrypting apparatus becomes simple.

[0036]

According to the present second invention, since the information inherent in the recording medium is information signal inherent for the recording medium to be recorded on the recording medium in the

encrypting method according to the present first invention, it is possible in addition to the effects of the present first invention to obtain encrypting method where the information signal inherent in the recording medium can be selected freely.

[0037]

According to the present third invention, since the information signal inherent for the recording medium to be recorded on the recording medium is random data to be inserted into a predetermined portion of the encrypted information data to be recorded on the recording medium in the encrypting method according to the present second invention, it is possible in addition to the effects of the present second invention to make it difficult to read the random data by dispersing the random-data insertion positions and the like and to obtain an encrypting method where a very strong copy protect on the information data can be effected.

[0038]

According to the present fourth invention, since a file of the encrypted information data and a file indicative of the portion of

random data to be inserted into a predetermined portion of the encrypted information data recorded on the recording medium are recorded on the recording medium in the encrypting method according to the present third invention, similar effects as the present third invention can be obtained.

[0039]

According to the present fifth invention, it is possible to obtain a decrypting method where an encryption key is obtained based on random data to be inserted into a predetermined portion of the encrypted information data to be recorded on a recording medium; a file of information data encrypted by the encryption key and a file indicative of the portion of random data inserted into a predetermined portion of encrypted information data recorded on the recording medium are reproduced from a recording medium recorded with the file of information data encrypted by the encryption key and the file indicative of a predetermined portion of random data inserted into a predetermined portion of encrypted information data recorded on the recording medium; the random data from the reproduced encrypted

information data are detected based on the reproduced file indicative of the portion of random data inserted into a predetermined portion of encrypted information data recorded on the recording medium; a decryption key is generated from the detected random data; and the encrypted information data of the reproduced information-data file are decrypted in a decrypting apparatus of a simple constitution by using the decryption key.

[0040]

According to the present sixth invention, since the information signal inherent in the recording medium to be recorded on the recording medium is a wobbling frequency of a predetermine portion of information data to be recorded on the recording medium in the encrypting method according to the present second invention, it is possible in addition to the effects of the present second invention to obtain an encrypting method where a very strong copy protect on the information data can be effected.

[0041]

According to the present seventh invention, since an encrypting

method characterized in that a file of the encrypted information data and a file indicative of the portion of the wobbling frequency to be inserted into a predetermined portion of the encrypted information data to be recorded on the recording medium are recorded on the recording medium in the encrypting method according to the present sixth invention, similar effects as the present sixth invention can be obtained.

[0042]

According to the present fifth invention, it is possible to obtain a decrypting method where an encryption key is obtained based on a wobbling frequency of a predetermined portion of information data to be recorded on a recording medium; a file of information data encrypted by the encryption key and a file indicative of a predetermined portion of encrypted information data to be recorded on the recording medium are reproduced from a recording medium recorded with the file of information data encrypted by the encryption key and the file indicative of a predetermined portion of encrypted information data to be recorded on the recording medium; a wobbling

frequency of a predetermined portion of the detected encrypted information data is detected based on the reproduced file of a predetermined portion of encrypted information data; a decryption key is generated from the detected wobbling frequency; and the encrypted information data of the reproduced encrypted information-data file are decrypted in a decrypting apparatus of a simple constitution by using the decryption key.

[0043]

According to the present ninth invention, since the recording medium is a recording medium of a disc shape and the information inherent in the recording medium is a physical information to be formed the recording medium in the encrypting method according to the present first invention, it is possible in addition to the effects of the present first invention to obtain an encrypting method where a very strong copy protect on the information data can be effected.

[0044]

According to the present tenth invention, since the physical information is a frequency of a predetermined portion of a wobbled

pre groove or a wobbled land portion to be formed on the recording medium in the encrypting method according to the present ninth invention, similar effects as the present ninth invention can be obtained.

[0045]

According to the present eleventh invention, since an encrypting method characterized in that the a file of the encrypted information data and a file indicative of a predetermined portion of a frequency at a predetermined portion of a wobbled pre groove or a wobbled land portion to be formed on the recording medium are recorded on the recording medium in the encrypting method according to the present ninth invention, similar effects as the present ninth invention can be obtained.

[0046]

According to the present twelfth invention, it is possible to obtain a decrypting method where an encryption key is obtained based on a frequency of a predetermined portion of a wobbling-shaped pre groove or a wobbling-shaped land portion to be formed on a recording

medium; the file of the encrypted information data and the file indicative of a predetermined portion of a wobbling-shaped pre groove or a wobbling-shaped land portion to be formed on a recording medium are reproduced from a recording medium recorded with a file of information data encrypted by using an encryption key and a file indicative of a predetermined portion of the wobbling-shaped pre groove or the wobbling-shaped land portion to be formed on a recording medium; the wobbling frequency of a predetermined portion of the pre groove or land portion formed on the recording medium is detected based on the reproduced file of a predetermined portion of the pre groove or land portion; a decryption key is generated from the detected wobbling frequency; and the encrypted information data are decrypted in a decrypting apparatus of a simple constitution by using the decryption key.

[0047]

According to the present thirteenth invention, since the random data is random data selected from a predetermined portion of a random file generated by a predetermined pseudo random generator in the

encrypting method according to the present third invention, it is possible in addition to the effects of the present third invention to obtain an encrypting method where a very strong copy protect on the information data can be effected.

[0048]

According to the present fourteenth invention, since a information-data file encrypted by the encryption key, a file indicative of the predetermined portion of the random file formed of the random data and the random file are recorded on the recording medium in the encrypting method according to the present thirteenth invention, similar effects as the present thirteenth invention can be obtained.

[0049]

According to the present fifteenth invention, since an encryption key is obtained based on random data selected from a predetermined portion of a random file generated by a pseudo random generator; a file of the encrypted information data, a file indicative of the predetermined portion of the random file from recording medium

recorded with a file of information data encrypted by the encryption key generated, and a file indicative of the predetermined portion of the random file are reproduced; a decryption key is generated from random data obtained from a file indicative of a predetermined portion of the random file of the reproduced random data and obtained from the random file; and the encrypted information data of a file of the reproduced encrypted information data are decrypted in a decrypting apparatus of a simple constitution by using the decryption key, it is possible to obtain a decrypting method where the information data are encrypted by the encrypting method according to the present fourteenth invention are decrypted in a decrypting apparatus of a simple constitution.

[0050]

According to the present sixteenth invention, since information data to be recorded on a recording medium are encrypted by using a first encryption key generated from information inherent in the recording medium and a third encryption key generated from a second encryption key independent of the first encryption key, the

constitution of the encrypting apparatus becomes simple, and it is possible to effect a very strong copy protect on the information data which is recorded on a recording medium and at the same time to obtain a decrypting method where the constitution of the decrypting apparatus becomes simple.

[0051]

According to the present seventeenth invention, since a first decryption key is generated from inherent information in a recording medium where encrypted information data are recorded by using a first encryption key generated from information inherent in the recording medium and a third encryption key generated from a second encryption key independent of the first key; a third decryption key is generated from a second decryption key obtained from a key medium provided with a second decryption key related to the second encryption key and from the first key; and the encrypted information data reproduced from the recording medium are decrypted by using the third decryption key, it is possible to obtain a decrypting method where the information data are encrypted by the encrypting method according to the present

sixteenth invention are decrypted in a decrypting apparatus of a simple constitution.

[0052]

According to the present eighteenth invention, since the key medium is a card where the second decryption key is recorded magnetically or optically in the decrypting method according to the present seventeenth invention, it becomes easy to handle and carry the key medium in addition to the effects of the present seventeenth invention.

[0053]

According to the present fourteenth invention, since the key medium comprises a memory storing the second decryption key in the decrypting method according to the present seventeenth invention, similar effects as the present seventeenth invention can be obtained.

[0054]

According to the present 20th invention, since the key medium is a card, it becomes easy to handle and carry the key medium in addition to the effects of the present seventeenth invention.

[0055]

According to the present 21st invention, since the key medium is a print medium where the second decryption key is printed in the decrypting method according to the present seventeenth invention, similar effects as the present seventeenth invention can be obtained.

[0056]

According to the present 22nd invention, since the print medium is a card in the decrypting method according to the present 21st invention, it becomes easy to handle and carry the key medium in addition to the effects of the present 21st invention.

[0057]

According to the present 23rd invention, since the print medium is the recording medium itself in the decrypting method according to the present 21st invention, it becomes unnecessary to provide the key medium separately from the recording medium in addition to the effects of the present 21st invention.

[0058]

According to the present 24th invention, since the recording

medium is a disc shaped recording medium in the encrypting method according to the present second invention, similar effects as the present second invention can be obtained.

[0059]

According to the present 25th invention, since the recording medium is a tape shaped recording medium, similar effects as the present second invention can be obtained.

[0060]

According to the present 26th invention, since the information data are video data, similar effects as the present second invention can be obtained.

[0061]

According to the present 27th invention, since the information data are audio data, similar effects as the present second invention can be obtained.

[Brief Description of Drawings]

[FIG. 1] is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus according to a first embodiment

of the present invention.

[FIG. 2] is a flowchart used to explain an encrypting operation of an encrypting apparatus according to the first embodiment of the present invention.

[FIG. 3] is a table showing an example of an arrangement of a digest method file.

[FIG. 4] is a diagram used to explain a method of producing a disc digest.

[FIG. 5] is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus according to a second embodiment of the present invention.

[FIG. 6] is a flowchart used to explain an encrypting operation of an encrypting apparatus according to the second embodiment of the present invention.

[FIG. 7] is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus according to a third embodiment of the present invention.

[FIG. 8] is a flowchart used to explain an encrypting operation of

an encrypting apparatus according to the third embodiment of the present invention.

[FIG. 9] is a flowchart used to explain a decrypting operation of a decrypting apparatus according to the third embodiment of the present invention.

[FIG. 10] is a diagram used to explain encrypting and decrypting methods employed by the encrypting and decrypting apparatus according to the third embodiment.

[FIG. 11] is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus according to a fourth embodiment of the present invention.

[Description of Reference Numerals]

1: encrypting apparatus

2: information data generating means

3: encrypting means

4: encryption-key generating means

5: recording medium inherent information generating means

6: file forming means indicative of predetermined portion of encrypted

information data.

7: recording means

8: hard disc

9: reproducing means

10: formatting means

11: recording means

12: master disc

13: disc producing apparatus

14: decrypting apparatus

15: disc

16: reproducing means

17: decrypting means

18: decryption-key generating means

19: output terminal

20: random file forming means

21: file forming means indicative of predetermined portion of random file

[Title of Document] Abstract

[Abstract]

[Problem]

[Solving Means]

ABSTRACT OF THE DISCLOSURE

When information to be recorded is encrypted by using an encryption key, an encryption key based on inherent information inherent in a recording medium is generated. The information to be recorded on the recording medium is encrypted based on the encryption key. The inherent information inherent in the recording medium is specific information on a disc. When an encrypted information recorded on a recording medium is decrypted, there are reproduced from a recording medium a first file storing information encrypted by using an encryption key generated based on a random data to be inserted into a predetermined portion of the encrypted information to be recorded on a recording medium and a second file storing data indicative of a predetermined portion of the random data to be inserted into a predetermined portion of the encrypted information. The

random data is detected from the encrypted information stored the reproduced first file based on the data stored in the reproduced second file and indicating the predetermined portion of the random data. A decryption key is generated from the detected random data. The encrypted information of the reproduced first file is decrypted by using the decryption key.

[Selected Drawing] FIG. 2